



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,188	07/02/2002	Dov Moran	10519/1167 (MSA-0019-2-US)	4688
67813 7590 09/14/2011 BRINKS HOFER GILSON & LIONE/SanDisk P.O. BOX 10395 CHICAGO, IL 60610				
EXAMINER				
TINKLER, MURIEL S				
ART UNIT		PAPER NUMBER		
3691				
MAIL DATE		DELIVERY MODE		
09/14/2011		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/089,188

Applicant(s)

MORAN ET AL.

Examiner

MURIEL TINKLER

Art Unit

3691

Period for Reply
-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 21 June 2011.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1, 4, 6-17, 51, 52 and 54 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1, 4, 6-17, 51, 52 and 54 is/are rejected.
- 8) ☒ Claim(s) 51, 52 and 54 is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-SB-005)
Paper No(s)/Mail Date 6/17/2010
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date ____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: ____

DETAILED ACTION

This application has been reviewed. The status of the claims are as follows: claims 1, 4, 6-17 and 51-54 were previously pending; claim 53 has been cancelled; claim 1 has been amended; no claims have been withdrawn or cancelled; therefore, claims 1, 4, 6-17 and 51-54 are currently pending and have been examined. The rejections are as follows.

Claim Objections

1. Claims 51, 52 and 54 are objected to because of the following informalities: claim 51, 52 and 54 are listed as "(New)" when in fact they should be listed as "(Previously Presented)". Appropriate correction is required.

Response to Arguments

2. Applicant's arguments, see page 7, filed June 17, 2010, with respect to the rejection(s) of claim(s) 1, 4 and 6-17 under 35 USC 101 and 35 USC 112 have been fully considered and are persuasive.

3. Applicant's arguments filed June 17, 2010 have been fully considered but they are not persuasive.

4. The Applicant argues, on pages 6-10 that the combination of Gullman, Helland, and Pare fail to each the following elements: "biometric interface for receiving, independently of the host device, a request to access the flash memory at the removable storage device" and the "processor for managing access to the flash

memory, independently of the host device, based on a comparison of the request to the at least one permission, the comparison being independent, requiring no management by an operating system of the host device, such that if the at least one permission includes a particular access type that matches the access requested in the request, the processor provides such access to the flash memory, and alternatively if the at least one permission does not include a particular access type that matches the access requested in the request, the processor denies such access to the flash.

5. The Examiner disagrees. Gullman discloses this in two distinct embodiments. See column 2, lines 27-39, which discloses an embodiment of the invention where the biometric security mechanism stores a template of user biometric information. In this embodiment, the biometric device generates a token to the user, who in turn accesses the host device using the token. However, this particular embodiment does not explicitly state that the biometric device is separate from the host device (it also does not disclose that it is directly connected). In a different embodiment disclosed in column 2, lines 47-65, Gullman states that the biometric device is an integrated circuit card including a processing unit, memory and a biometric sensor. Finally, the Examiner has used Helland in the Office Action mailed on March 17, 2010 with regard to the use of flash memory.

6. In response to applicant's argument, on pages 7-10, that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., managing access to the host system) are not recited in the rejected claim(s). Instead, what is disclosed in the claim language is "communication with the

USB bus of the host device". Also disclosed in the claims language is "managing access to the flash memory". The Examiner further points out that the flash memory is in the removable storage device, not the host. Additionally, the claim language discloses that the removable storage device requires "no management by the operating system of the host device". So, the claim does disclose: that the host device is not required to access the flash memory; and, communicates with the host device. The claim does NOT disclose that the biometric device is "managing" access to the host system. Finally, the Examiner points out that: Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

7. Regarding the argument, on pages 8-9, stating the cited prior art does not disclose a processor of a removable storage device independently determining whether to grant a user access to flash memory of the storage device without management from a host device. The Examiner disagrees. Gullman discloses this in column 2 (lines 27-65). A portion of this section has been copied below:

" In an exemplary embodiment of the invention, the biometric security mechanism is an integrated circuit card including a processing unit, memory and a biometric sensor. The memory stores a template of the authorized user's biometric information, along with a verification algorithm. Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number) and time-varying self-generated information to derive a token output. The token output is displayed on the card where the cardholder can view the token and manually enter the token to an access device coupled to the host system. In an alternative embodiment, the token output is transmitted directly to the host system through a direct data communication line, eliminating the need for manual entry by the user."

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claim 1-9, 12, 14-17 and 51-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullman et al. (US 5,280,527) in view of Helland et al. (US 6,014,666), hereafter referred to as Gullman and Helland.

11. Regarding claims 1 and 51 and 52, Gullman discloses:

- a. A method and device for controlling access to a resource, access being provided through a host device, the device (see Abstract)
- b. an input for receiving a request to access the resource (figure 1 #14—biometric security sensor); and,

- c. a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided (see figure 2 #22—processor and column 2, lines 27-65);
 - d. a biometric interface (see figure 1, element 14 “sensor”; figure 2, element 18; and figure 2, element 18).
 - e. determining permission of the user, via a biometric security apparatus (figure 1, element 14), and stored memory (figure 2, element 22), without any type of management from an operating system of the host device (see column 2, lines 20-65; and, column 5, line 57 through column 6, line 29).
 - f. Denying access, see column 2 (lines 37-55)
12. Gullman does not disclose a USB and a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor; a flash memory device for storing at least one permission for determining access to the resource; and, a flash memory controller for controlling said flash memory device. Helland discloses these things in column 5 (line 55) through column 6 (line 5) and column 6 (lines 13-27). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Gullman to include the use of flash memory and universal serial bus because both flash

and universal serial bus were well known in the art as storage and connectivity options at the time the invention was made.

13. Regarding claim 4, Gullman discloses: The storage system of claim 1, wherein said biometric detection device further comprises: a sample collector for collecting said biological parameter of the user (see column 3 (lines 36-55)).

14. Regarding claim 6, Gullman discloses: The storage system of claim 4, wherein said biological parameter of the user is a fingerprint of the user (see column 3 (lines 36-55)).

15. Regarding claim 7, Gullman discloses: The storage system of claim 1, further comprising: (f) a RAM component for storing data for performing said at least one instruction of said data processor (see figure 2 #33).

16. Regarding claim 8, Gullman discloses: The storage system of claim 1, further comprising: (f) a cryptographic chip for encrypting and decrypting data (see figure 3).

17. Regarding claim 9, Gullman discloses: The storage system of claim 8, wherein said cryptographic chip performs an authentication process (see column 4 (line 50) through column 5 (line 14) and column 5 (lines 34-39)).

18. Regarding claim 12, Gullman discloses: The storage system of claim 8, wherein said cryptographic chip performs encryption immediately upon receiving a command from said data processor (real-time, see column 4 (line 50) through column 5 (line 14)).

19. Regarding claims 14 and 15, Gullman discloses: The storage system of claim 8, wherein said cryptographic chip further comprises a cryptographic chip memory for storing at least one cryptographic key and at least one cryptographic instruction for

encrypting and decrypting data, such that said cryptographic chip forms a removable encryption engine; wherein said encrypted data is stored on said cryptographic chip memory (see figure 2 #33).

20. Regarding claims 17, Gullman discloses: the storage system of claim 15, wherein said cryptographic chip memory is said flash memory device (see the rejection of claim 1 above).

21. Regarding claim 16, The Examiner argues that it would be obvious make something separate that is currently combined (see the rejection of claim 17 above).

22. Regarding claim 53, which states, “wherein the access control module is distinct from a removable storage device comprising the flash memory”. However, based on the reasoning above, the Examiner will interpret this claim as an access control device connected to a removable storage device. Gullman discloses this in the Abstract and column 2 (lines 21-27).

23. Regarding claim 54, Gullman discloses:

- a. An access control device configured to communicate with a host device, the access control device comprising: a biometric interface (see Abstract, figure 1, element 14 “sensor”; figure 2, element 18; and figure 2, element 18)
- b. for receiving, independent of the host system, a request at the access control device to access a flash memory (figure 1 #14—biometric security sensor); and
- c. a processor for managing access to the flash memory independent of the host device based on a comparison of the request to at least one permission, the

comparison being independent of, and requiring no management by an operating system of the host device, such that if the at least one permission includes a particular access type that matches the access requested in the request, the processor provides such access to the flash memory (figure 1, element 14), (figure 2, element 22), see column 2, lines 20-65; and, column 5, line 57 through column 6, line 29), and

d. alternatively if the at least one permission does not include a particular access type that matches the access requested in the request, the processor denies such access to the flash memory, see column 2 (lines 37-55).

24. Gullman does not disclose a USB and a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor; a flash memory device for storing at least one permission for determining access to the resource; and, a flash memory controller for controlling said flash memory device. Helland discloses these things in column 5 (line 55) through column 6 (line 5) and column 6 (lines 13-27). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Gullman to include the use of flash memory and universal serial bus because both flash and universal serial bus were well known in the art as storage and connectivity options at the time the invention was made.

25. Claims 10, 11 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Gullman and Helland as applied to claims 8 and 12 above, and further in view of Pare et al. (US 5,805,719), hereafter referred to as Pare.

26. Regarding claims 10 and 11, Gullman and Helland disclose the information in claim 8. Gullman and Helland do not disclose that said cryptographic chip emulates a smart card and stores encrypted smart card data. Pare discloses this in column 2 (line 24) through column 3 (line 14). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Gullman and Helland to include the use of a smart card and encrypted smart card data because it is a current was an increasing trend in the banking industry at the time of this invention and it provides an efficient way to store information.

27. Regarding claim 13, Gullman and Helland disclose the information in claim 12. Gullman and Helland do not disclose that said cryptographic chip creates a cryptographic signature with a hash immediately upon receiving a command from said data processor. Pare discloses the use of a hash algorithm in column 62 (line 62) through column 63 (line 10). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Gullman and Helland to include a hash algorithm because it provides further security for data that may travel through an un-secure network.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MURIEL TINKLER whose telephone number is (571)272-7976. The examiner can normally be reached on Monday through Friday from 8 AM until 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Alexander Kalinowski can be reached on (571)272-6771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Muriel Tinkler/
Primary Examiner, Art Unit 3691